Cyber bank robbery

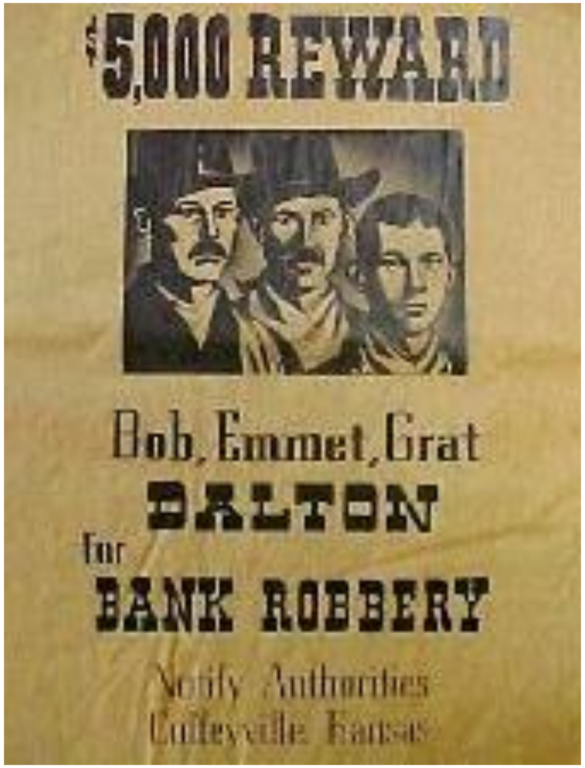
Erik Poll

Digital Security

Radboud Universiteit Nijmegen

Banks & (cyber) crime

Banks a long-time favourite target of criminals



Also of *cyber* criminals

- Some anecdotes & historical trends
- What can we learn from this?

Bangladesh Central Bank heist

- Attempt to steal $ 951 million using SWIFT global payment system
  - Most of money recovered
  - $ 81 million moved to casinos in the Philippines
- Attackers installed custom malware showing inside knowledge
  - to remove validity checks
  - to delete transactions from local database & physical print-outs

These are not script kiddies…

[http://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html]

[http://www.reuters.com/assets/iframe/cmsyovideo?videoId=370707923]

[https://www.nettitude.com/wp-content/uploads/2016/12/Nettitude-SWIFT-Threat-Advisory-Report-client.pdf]

Less ambitious attacks: skimming

- Mag-stripe on bank card contains digitally signed information

- but… this info can be copied

Skimming equipment

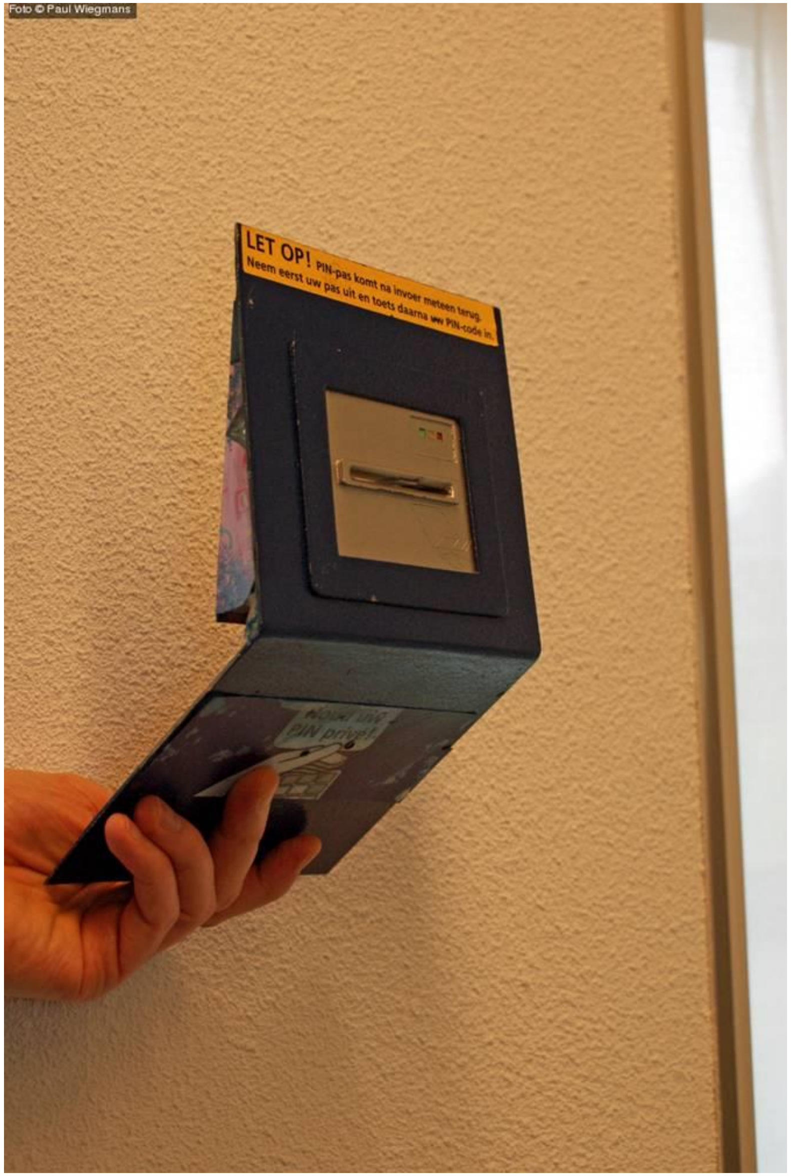
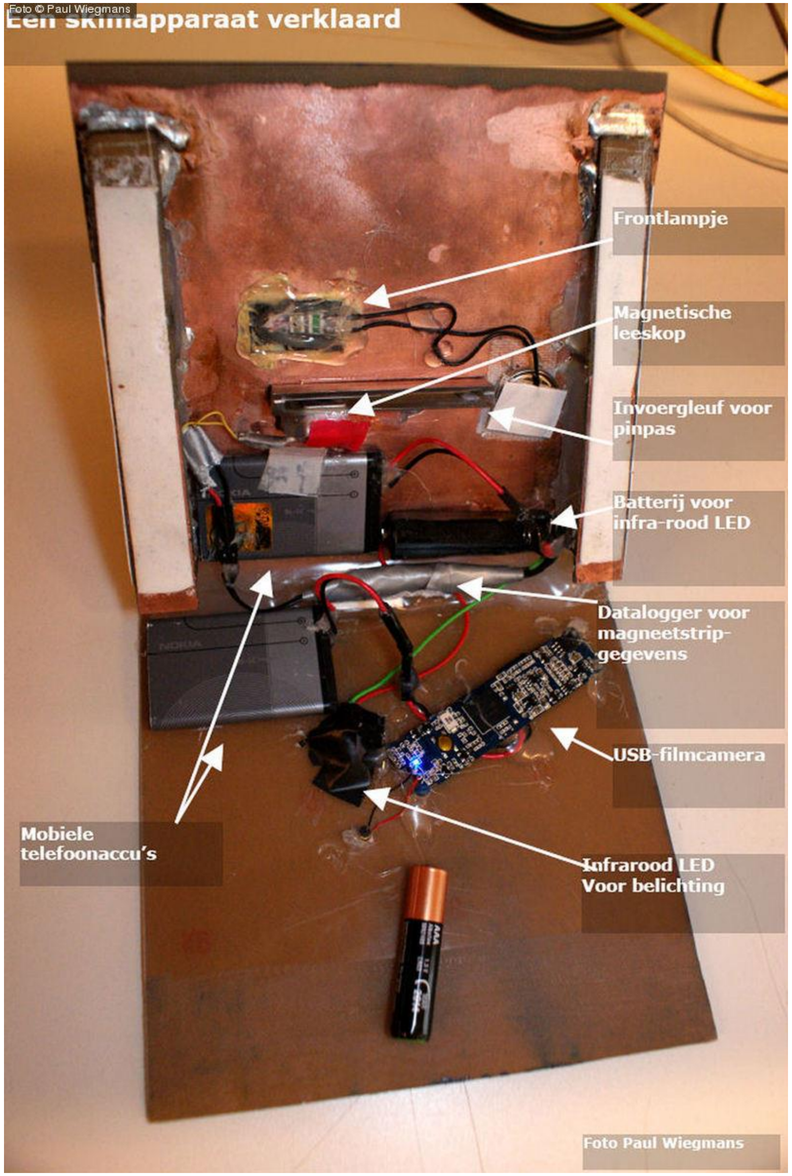
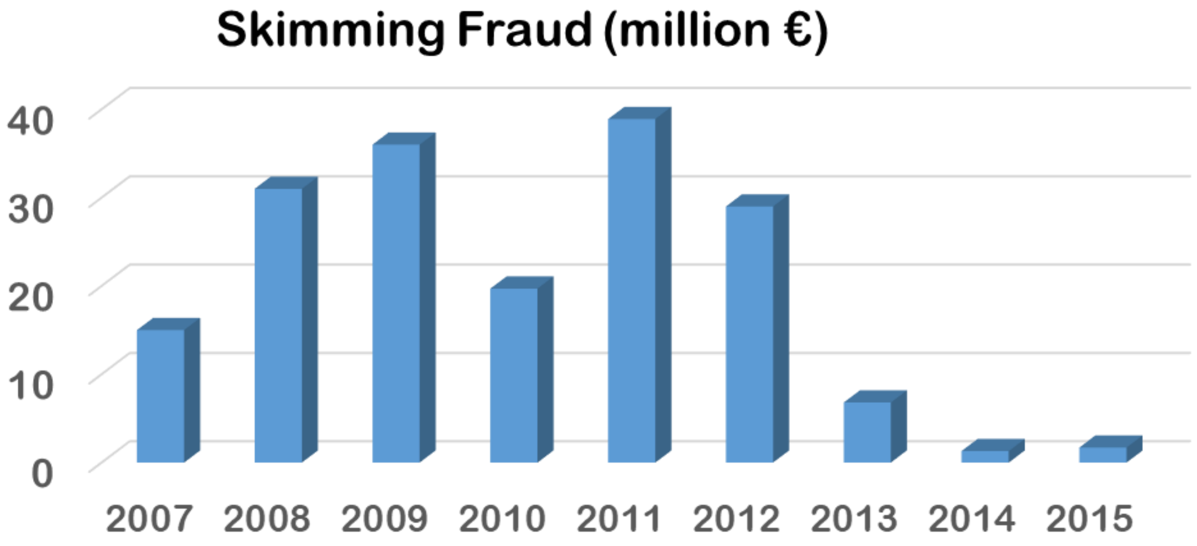


Foto © Paul Wiegmans
LET OP! PIN-pas komt na invoer meteen terug.
Neem eerst uw pas uit en toets daarna uw PIN-code in.



Skimming fraud in the Netherlands



[Source: NVB & Betaalvereniging]

Fraud reduced by

- better monitoring and response (blocking of cards)
- replacing magnetic stripe by EMV chip

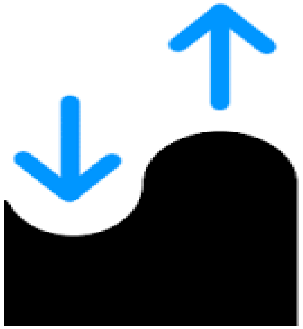
Does EMV chip reduce skimming?

- UK introduced EMV in 2006

	2005	2006	2007
domestic	79	46	31
foreign	18	53	113

Skimming fraud with UK cards, in millions £ [Source: UK Payment Association]

- Copied magstripes can still be used in countries don't use the chip…
  - Geoblocking is an effective countermeasure here
- Skimmers have now moved to the US,
  and US is now (slowly) migrating to EMV chips
- Such water bed effects are a recurring phenomenon

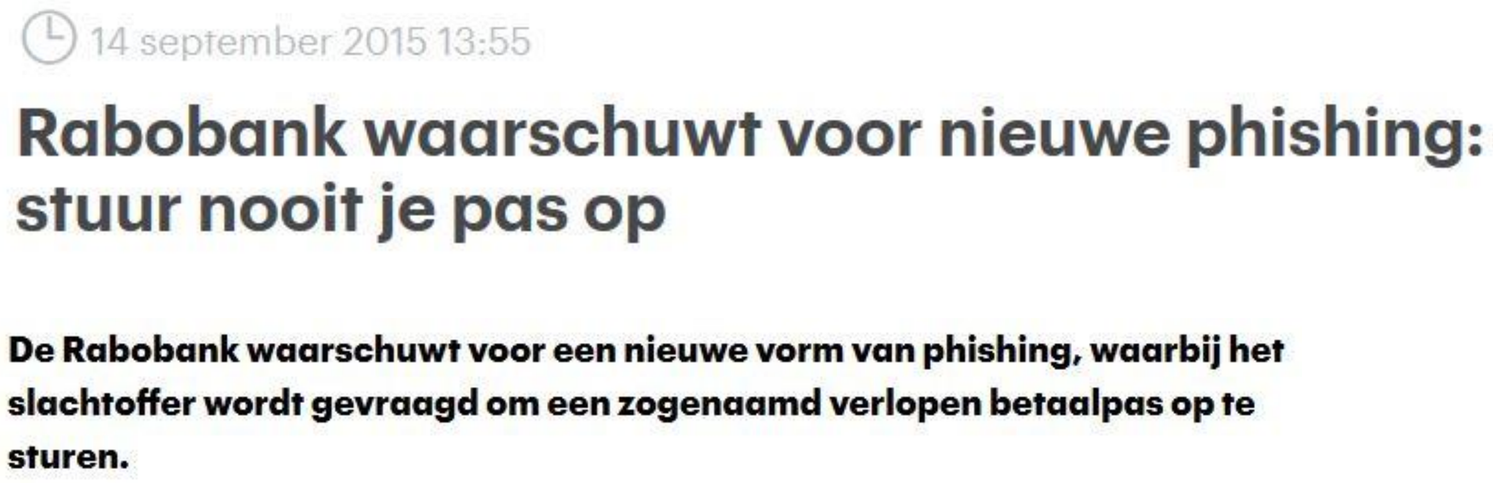


Recurring problem: backward compatibility

- In 2009, criminals put tampered card readers *inside* ABN-AMRO bank branches to skim cards
  - For *backward compatibility*, the chip reports the same data as is on the magstripe
  - Both magstripe data and PIN code are sent plaintext from card to reader
  - Criminals caught & convicted in 2011

- Cards have been improved to avoid this: magstripe data should now be different from info on the chip

More low-tech attacks

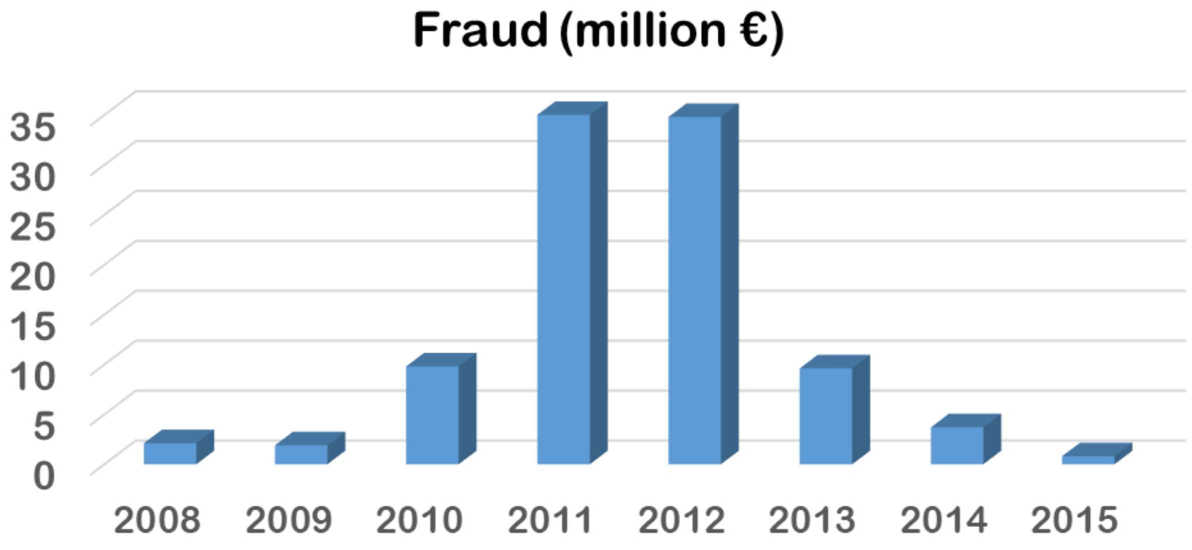


14 september 2015 13:55

Rabobank waarschuwt voor nieuwe phishing: stuur nooit je pas op

De Rabobank waarschuwt voor een nieuwe vorm van phishing, waarbij het slachtoffer wordt gevraagd om een zogenaamd verlopen betaalpas op te sturen.

Internet banking fraud in Netherlands

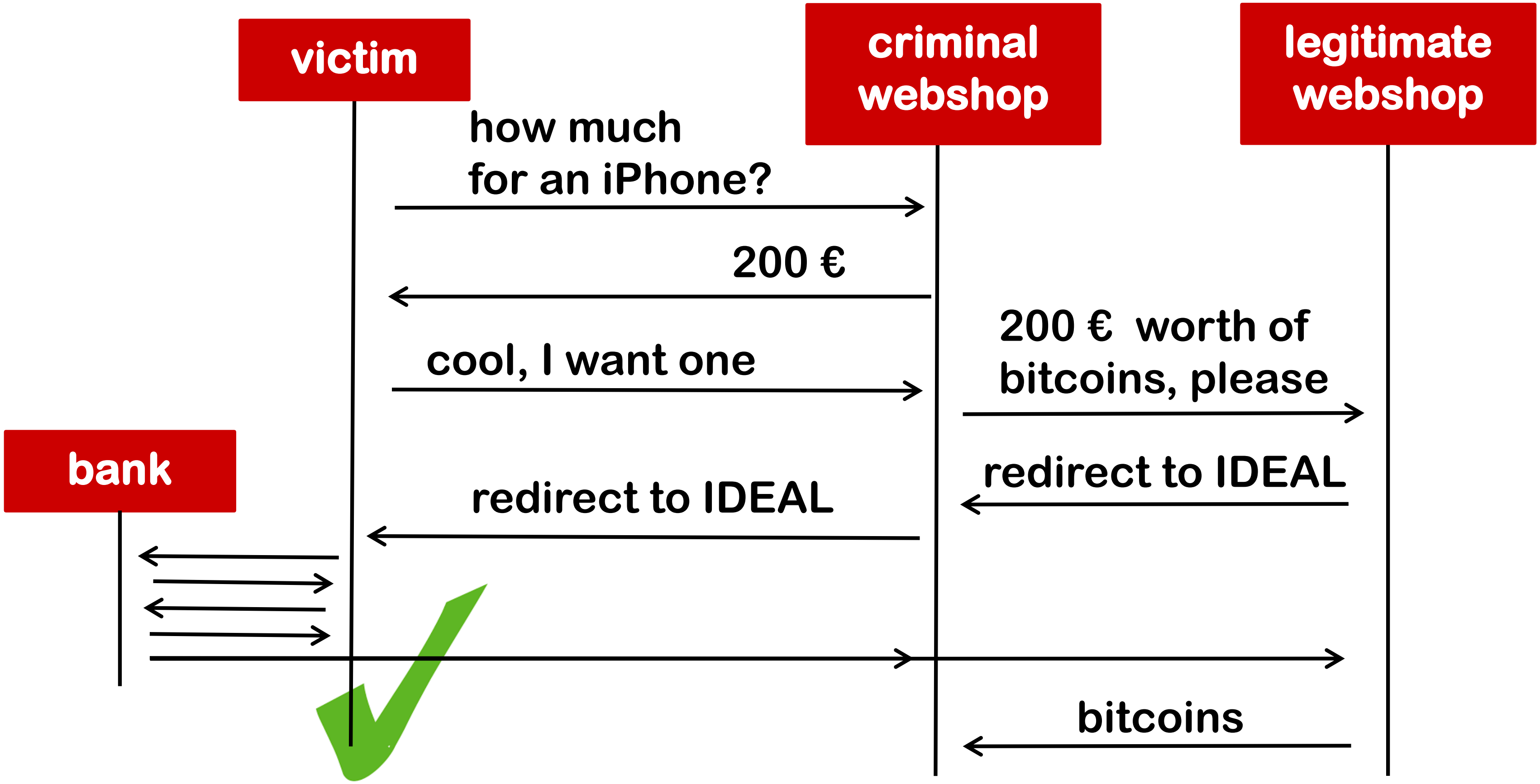


[Source: NVB & Betaalvereniging]

Fraud reduction through

- better monitoring - for fraudulent transactions & money mules
- awareness campaigns
- criminals moving to ransomware as better business model?

Example attack on IDEAL



- Root cause: messages to the user (about some 3rd party payment service provider) not very informative, so hard to spot this fraud
- IDEAL now monitors payments to bitcoin shops & online gambling sites

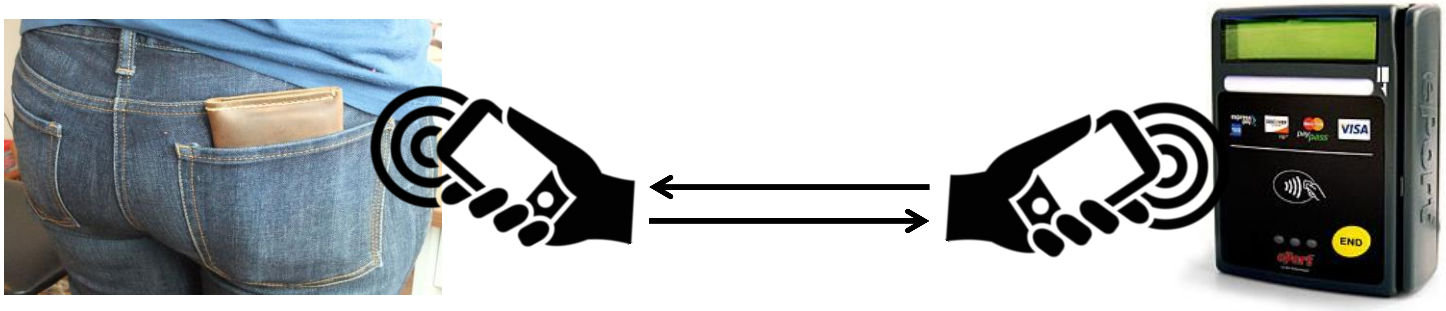
Contactless payments)))

Contactless version of EMV with contactless card or NFC mobile phone

- ***Who here uses a metal wallet to protect their contactless card?***
- ***Who thinks contactless payments without PIN are less secure than contact payments with PIN?***

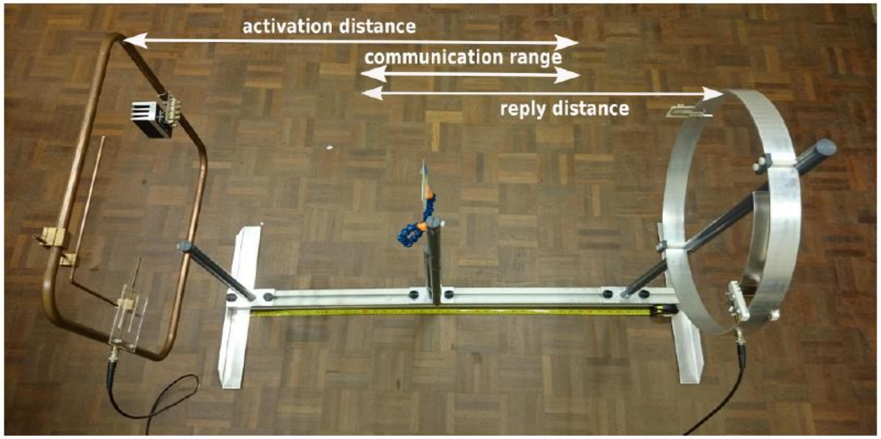
Security of contactless cards

- It is *not* possible to clone a contactless card
- It *is* possible to do a 'live' relay attack with a contactless card



•Is there a good criminal business model for relay attacks?

- Max distance for activating contactless card is ≈ 40 cm



[René Habraken et al., An RFID Skimming Gate Using Higher Harmonics, RFIDSec 2015]

Risks of contact vs contactless cards

1. Risks of contactless payments *without* PIN

   a) I can loose 50 euro max. if my card is stolen`.

   b) I can loose 25 euro max. if I fall victim to an (unlikely) relay attack.

   These losses may be refunded by the bank.

2. Risks of contact payments *with* PIN

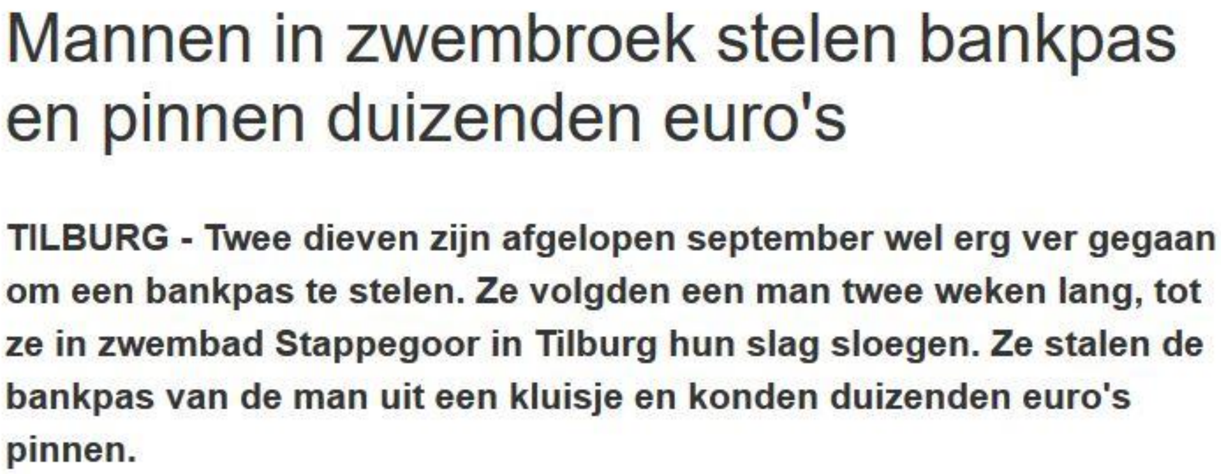
   a) I won't loose any money if my card is stolen.

   b) I can loose 1000s of euros if my card stolen & my PIN code is seen.

   These losses are less/unlikely to be refunded by the bank.

The 'extra security' of the PIN code *increases* risks to the user.

NB technical security weakness $\neq$ risk



Mannen in zwembroek stelen bankpas en pinnen duizenden euro's

TILBURG - Twee dieven zijn afgelopen september wel erg ver gegaan om een bankpas te stelen. Ze volgden een man twee weken lang, tot ze in zwembad Stappegoor in Tilburg hun slag sloegen. Ze stalen de bankpas van de man uit een kluisje en konden duizenden euro's pinnen.

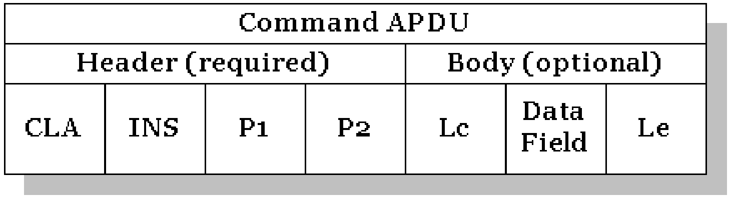
**[Bron: omroepbrabant.nl,
https://www.youtube.com/watch?v=tpVTdj6xg3c]**

Oops: buffer overflows….

Contactless payment terminals of one vendor crashed on unusual - but legal - inputs.

[Jordi van den Breekel, *A security evaluation and proof-of-concept relay attack on Dutch EMV contactless transactions*, MSc thesis, 2014]

- Could you exploit this in more interesting ways, eg. to get malware on the payment terminal?
- Is the same software stack in their other terminals, eg. their ATMs?
- The input format for smartcard terminals is *extremely* simple.
  - How can you implement this wrong?
  - If you do, how can your tests miss it?



Command APDU						
Header (required)				Body (optional)		
CLA	INS	P1	P2	Lc	Data Field	Le

Apparently compliance tests like emv CERTIFIED *are not checking for such basic software security flaws?*

Oops: configuration flaws...

Mistake on the first generation contactless cards issued in the Netherlands:

Functionality to check the PIN code,

which should only be accessible via the contact interface

was also accessible via the contactless interface

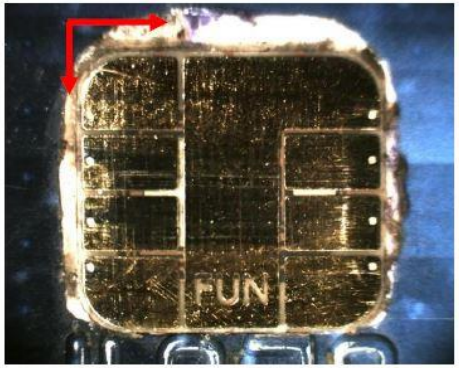
Possible risk for DoS attacks, rather than financial fraud.

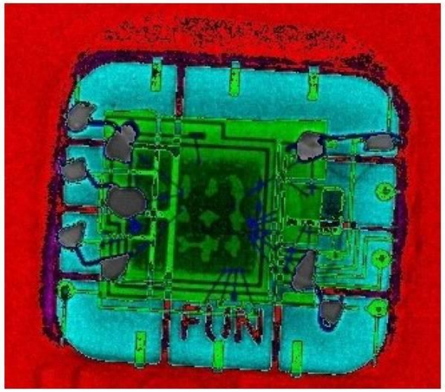
This was a known weakness from the UK; why did nobody spot this?

Flaw discovered bij Radboud University students Anton Jongsma, Robert Kleinpenning, and Peter Maandag.

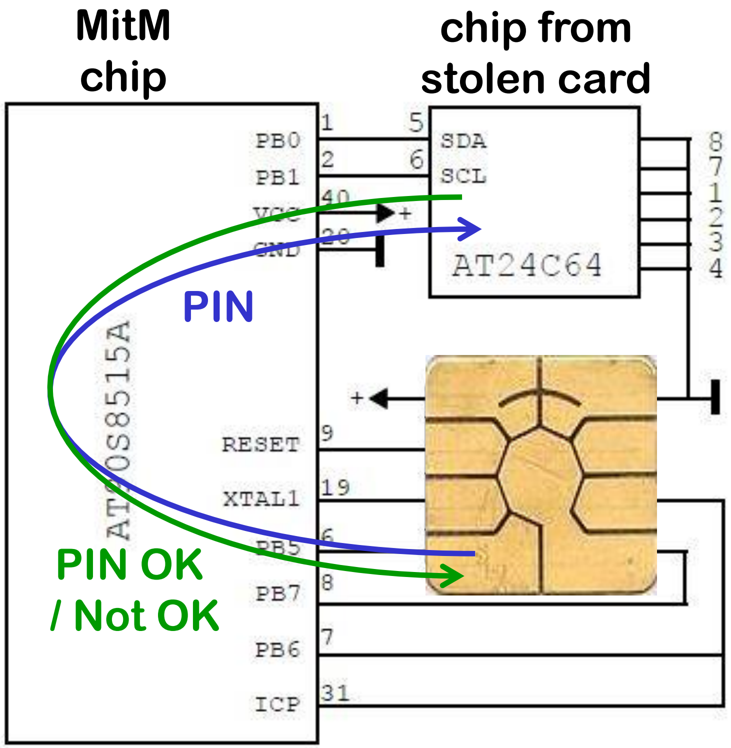
Hi-tech attack with stolen cards

Chips from stolen cards inserted under another chip,
for Man-in-the-Middle attack to fake the PIN verification response





xray reveals
green stolen chip under
blue microcontroller



MitM chip

chip from stolen card

PIN

PIN OK / Not OK

PIN verification response of the card to terminal is not authenticated

[Houda Ferradi et al., *When Organized Crime Applies Academic Results: A Forensic Analysis of an In-Card Listening Device*, Journal of Cryptographic Engineering, 2015]

Conclusions

Why banking security is easy!

- Banks can measure and quantify attacks in euros
  - Trends in attacks can be followed
  - Success of defensive measures can be measured
  - This provides rational basis for security decisions

- In other industries this is *MUCH* harder!
  - Eg for critical infrastructures or hospitals:
    How much can cyber protection of the electric grid cost?
    Or patient privacy?

  Ransomware may play a “useful” role here…

Conclusions

- General trend: from prevention to better detection & response
- Technical security flaws are not always serious security risks;
  The real issue: can attacker find a good business model?
  - The bad news here: ransomware is a great business model for almost any security weakness
- Some silly flaws in products from reputable companies & vendors
  - Who is *really* taking the responsibility for the security?
    - Banks, vendors, 3rd parties doing certification,
      Mastercard, Visa, or EMVco, who also approve vendors & certifiers
  - How much security is just Cover-Your-Ass security?

Thanks for your attention